

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, on behalf of
its agencies, DEPARTMENT of the NAVY,
THE DEFENSE THREAT REDUCTION
AGENCY, THE UNITED STATES NUCLEAR
SECURITY ADMINISTRATION, and the
FEDERAL BUREAU OF INVESTIGATION,

PLAINTIFFS,

KITSAP COUNTY and the KITSAP COUNTY
DEPARTMENT OF EMERGENCY
MANAGEMENT,

DEFENDANTS.

CASE NO.

DECLARATION OF CAPTAIN
THOMAS W. ARMSTRONG

I. INTRODUCTION AND QUALIFICATIONS

1. I am the Nuclear Weapons Surety/Policy and Compliance Branch Head for the Strategic Systems Programs (SSP). I have held this position since December 2009. In this position, I report directly to the senior advisor to the Director of SSP (DIRSSP) on nuclear weapons safety and security. Additionally, I am responsible for overseeing all aspects of the SSP Nuclear Weapons Surety/Policy and Compliance. My responsibilities include recommending certification of all shore-based Navy nuclear weapons facilities for operations, and training and qualifying all Navy nuclear weapons inspectors on all facets of nuclear weapons safety, security, and procedural compliance.

4. The statements made in this declaration are based upon my personal knowledge or upon information available to me in my official capacity and are true and correct to the best of my knowledge and belief.

A. SSP's Mission

5. SSP ensures the operability and reliability of the Navy's TRIDENT II D5 fleet ballistic missile (TRIDENT missile) system. SSP is responsible for all operations and the mission requirements on its installations, including security, force protection, and explosives safety. The Navy's TRIDENT program includes the OHIO Class Ballistic Missile submarines, TRIDENT missiles, and the specialized infrastructure that supports every aspect of the TRIDENT program operations, services and systems. This specialized infrastructure includes physical infrastructure, such as TRIDENT missile storage and handling facilities at SSP's Strategic Weapons Facility, Pacific on Naval Base Kitsap (SWFPAC), as well as the specialized security systems, which are composed of highly trained personnel, assets, and equipment designed to protect physical infrastructure. SWFPAC security force personnel transport TRIDENT missile components on convoy routes from onshore storage facilities to the waterfront restricted area, where TRIDENT missiles and assets are mated and then loaded onto Ohio Class submarines.

1 6. To prepare for a radiological incident or accident, and to ensure the safe transit of
2 TRIDENT missiles and warheads, on Naval Base Kitsap, SWFPAC security and technical personnel
3 participate in Nuclear Weapons Accident Incident Exercises (NUWAIX) and the Nuclear Weapon
4 Incident Response Training Program (NWIRT Program). NUWAIX and the NWIRT Program are
5 mechanisms for exercising the United States' interagency, state, and local cooperation and
6 collaboration in response to a radiological incident or accident. Effective coordination requires the
7 sharing of records containing sensitive incident response force information with various federal, state,
8 and local government agencies, including personnel from Commander, Navy Region Northwest
9 (CNRNW), the Defense Threat Reduction Agency (DTRA), the United States Coast Guard, the
10 Federal Bureau of Investigation (FBI), the Department of Energy, the Federal Emergency
11 Management Agency and the Kitsap County Department of Emergency Management (the County).

12 7. The incident response force is comprised of personnel that participate in NUWAIX
13 and the NWIRT Program, and its mission is to coordinate the DoD and interagency response assets to
14 recover weapons, save lives and protect individuals and property from health or safety hazards that
15 may result from a radiological incident on, or in the vicinity of Naval Base Kitsap and in U.S.
16 territorial waters. This includes all aspects of consequence management, site remediation and support
17 of other federal, state and local agency response efforts throughout all phases of the response to
18 include support to the FBI during recapture and recovery operations. The incident response force
19 must be prepared to deploy on short notice in response to any radiological incident or accident,
20 ranging from the most likely scenario, involving accidental damage to a weapon, to the most
21 dangerous scenarios, involving intentional threats to the weapons, such as terrorist seizure or
22 unauthorized detonation. The incident response force consists of first responders, including
23 specialized radiological response teams, explosive ordnance disposal teams, emergency fire and
24 medical services, and highly trained security forces. The response force also includes specialized
25 command and control units that coordinate the response over an extended period of time.

26 8. In addition to ensuring the physical security of the TRIDENT program, SSP is also
27 responsible for protecting sensitive information pertaining to the TRIDENT program. This
28 information includes DoD Unclassified Controlled Nuclear Information (UCNI), 10 U.S.C. § 128,
and Critical Infrastructure Security Information (CISI), 10 U.S.C. § 130e.

1 9. UCNI is defined under 10 U.S.C. § 128, as information that could reasonably be
2 expected to have a significant adverse effect on the health and safety of the public or the common
3 defense and security by significantly increasing the likelihood of the illegal production of nuclear
4 weapons or the theft, diversion, or sabotage of DoD Special Nuclear Material (SNM), SNM
5 equipment, SNM facilities, or nuclear weapons in DoD custody (referred to as the “adverse effects
6 test”). In order to protect information under 10 U.S.C. § 128, it must meet the adverse effects test and
7 fall within at least one of the categories of UCNI delineated in 32 C.F.R. § 223.7(c).

8 10. SSP has sole authority to designate specific unclassified information as DoD UCNI for
9 the TRIDENT program. Department of the Navy (DON) guidance for identifying and protecting
10 UCNI is provided in SECNAV M-5510.36, Department of the Navy Information Security Program,
11 and OPNAVINST 5513.5C [SCG 05-27.6], Submarine Launched Ballistic Missile (SLBM) Weapon
12 System Security Classification Guide (SCG). The SLBM SCG identifies classification levels, topics
13 of information and the reasoning used to determine whether documents and materials may be
14 designated as Classified, UCNI, or Unclassified. It is used as a reference by SSP’s nuclear weapons
15 security experts to identify information that must be protected as DoD UCNI. Information such as,
16 but not limited to, plans, procedures, and equipment for the protection of the TRIDENT missile
17 system is designated as DoD UCNI. For reasons of national security, information marked as UCNI
18 cannot be made publically available.

19 11. CISI is defined under 10 U.S.C. § 130e, as information that, if disclosed, would reveal
20 vulnerabilities in DoD critical infrastructure that, if exploited, would likely result in the significant
21 disruption, destruction, or damage of or to DoD operations, property, or facilities, including
22 information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines,
23 related to critical infrastructure or protected systems owned or operated by or on behalf of the DoD,
24 including vulnerability assessments prepared by or on behalf of the DoD, explosives safety
25 information (including storage and handling), and other site-specific information on or relating to
26 installation security. Information that meets this definition may be exempted from public release by
27 the DoD Director of Administration and Management (DA&M), upon a written finding that the
28 public consideration in disclosing the information does not outweigh preventing the disclosure. In
determining whether to exempt information as CISI, DoD(DA&M) relies upon DoD components,
such as SSP, to make initial threshold determinations as to whether information pertaining to their

1 program meets the definition of CISI, and to provide a written statement of the harm that would likely
2 result if the information were released. Within the DON, these threshold determinations are
3 submitted to DoD(DA&M) by the Department of the Navy Chief Information Officer, upon written
4 request by a DON component.

5 **B. The Washington Public Records Act Request**

6 12. On January 15, 2015, the County received a request from Glen Milner under the
7 Washington Public Records Act (PRA) for records pertaining to the consequences of a radiological
8 accident or similar event on Naval Base Kitsap-Bangor and other facilities owned or operated by the
9 Navy, and the emergency responses for such an event. On April 29, 2015, the County notified the
10 Navy about the PRA request and advised that the responsive records would be released unless the
11 federal government obtained a court order enjoining the release of the requested records. It is my
12 understanding that among the records responsive to Mr. Milner's request are documents regarding
13 several NUWAIX conducted in Kitsap County and training conducted under the NWIRT Program,
14 which contain information pertaining to convoy routes and incident response force personnel, assets,
15 and equipment.

16 13. This declaration serves two main purposes: (1) to outline the process used by SSP to
17 identify and redact sensitive information, including Controlled Unclassified Information (CUI) such
18 as UCNI and CISI, from documents responsive to the PRA request, and (2) to explain the harm that
19 would result if this information were released to the public.

20 **III. PROCESS**

21 14. On May 18, 2015, in response to a request from CNRNW, the County provided
22 approximately 6,000 pages of information to the Navy for review. Although CNRNW is technically
23 the originator of most of these records, it determined that the records included information generated
24 by other federal agency stakeholders, such as SSP and DTRA. Consequently, CNRNW notified SSP
25 of the records request to the County on May 19, 2015, and forwarded a subset of records for a
26 preliminary review to determine whether further review would be necessary. Based upon the
27 preliminary review, SSP determined that some of the documents contain information that should be
28 protected as CUI, and further review was necessary.

1 15. After SSP and other stakeholders communicated the results of the initial reviews,
2 CNRNW forwarded the full set of responsive records provided by the County to SSP and other
3 potential stakeholders, including DTRA. SSP assembled a team of security specialists, including SSP
4 staff and contractors (the CUI Team), to conduct a thorough review of the records. As outlined
5 above, SSP was chosen for this task because it has substantial experience with technical operations
6 and security, and information protection pertaining to nuclear weapons.

7 16. Personnel from one of SSP's contractors who are familiar with CUI conducted an
8 initial review, which was followed by an independent quality control review by government
9 personnel within SSP. Following the quality control review, the government and contractor
10 personnel discussed their assessments and reached a final determination. Any documents containing
11 CUI, as determined by the CUI Team, were redacted. Later, after CNRNW and DTRA completed
12 their own reviews, DoD and Navy stakeholders conducted a final reconciliation review. Once
13 reconciliation was completed, CNRNW compiled a Vaughn Index based upon the conclusions of the
14 DoD and Navy stakeholders.

15 **IV. HARM FROM RELEASE OF INFORMATION**

16 17. There is potential for substantial harm to the Navy if certain information in the records
17 within the County's possession were released in response to a PRA request. Specifically, the records
18 identified in the attached index contain sensitive information that, if released, would negatively
19 impact national security because release of such information could impact the Navy's ability to
20 ensure the operability, reliability, safety and security of the TRIDENT missile system, which the
21 United States relies heavily upon as a strategic deterrent. For the purposes of this declaration, the
22 harm that would result from the release of the sensitive information can be described in relation to
23 two general categories: (1) convoy route information and (2) incident response force information.
24 SSP has reviewed all of the records listed in the attached index and determined that each document on
25 this index contains information that fits into at least one of these two categories. As such, each record
26 listed on the attached index has been determined by SSP to contain UCNI and CISI.
27
28

A. Convoy Route Information

18. The first category of information marked as UCNI and CISI includes TRIDENT missile convoy route information. Convoy route information describes the path of movement that security forces use to transport TRIDENT missiles between storage facilities and the platform. Specific information describing the route, including street names and surrounding terrain, is considered convoy route information. If exploited, this information could provide a potential adversary with information that would allow it to determine how and where to most effectively execute an attack. Consequently, if convoy route information is released, it will negatively impact national security because it could impact the Navy's ability to ensure the operability, reliability, safety and security of the TRIDENT missile system.

19. Some of the documents containing convoy route information include the following: Document 19, Mini-NUWAIX 2014-01 Final Planning; Document 21, REGCOM Table Top Exercise 2014-02 SLIDES; Document 31, Task Force TTX Nov 13 Final Planning Conf slides; Document 42, NUWAIX15 Initial Planning Meeting. Specifically, for example, document 42 contains an image showing the location of the convoy route at Naval Base Bangor, Kitsap. See document 42, slide 44.

20. The convoy route information in these documents qualifies as two different categories of UCNI under 32 C.F.R. § 223.7(c). It constitutes a "Facility Description" under 32 C.F.R. § 223.7(c)(3) and provides "Threat Response Capability and Procedures" under 32 C.F.R. § 223.7(c)(6). Additionally, the convoy route information in such documents meets the adverse effects test under 10 U.S.C. § 128, because convoy route information could provide an adversary with the specific route by which a nuclear weapon or special nuclear material will be transported on DON property, which could enable an adversary to develop plans for an attack that would circumvent U.S. security infrastructure (including personnel, assets, equipment, and facilities), and impede response assets.

21. Convoy Route information also meets the definition of CISI, under 10 U.S.C. § 130e, and should be protected because the public interest considerations in disclosing this information are strongly outweighed by the harm. There is no public interest consideration that, on balance, would outweigh the significant harm that could result from disclosing convoy route information. The Navy already makes TRIDENT missile handling information publicly available to the extent it can without

1 | jeopardizing public health and safety, including the fact that it transports and handles TRIDENT
 2 | missiles on Naval Base Kitsap. Releasing the exact route that the convoy takes between two points
 3 | on the installation, or details pertaining to that route, would only serve to benefit the interests of those
 4 | wishing to cause harm to the public. Based on this determination, DON has submitted a request to
 5 | the DoD(DA&M) for a formal determination that the information is CISI, and therefore, remains in
 6 | the control of DON. As of the date of signing of this declaration we anticipate the CISI process to be
 7 | completed by late January.

8 | **B. Incident Response Force Information**

9 | 22. The second category of information marked as UCNI and CISI is incident response
 10 | force information. It includes information about the personnel, assets and equipment relied upon to
 11 | respond to a radiological accident or incident. It may describe, for example, the exact location of
 12 | incident response force personnel, assets and equipment; or incident response force capabilities, such
 13 | as quick reaction force response windows. If exploited, this information could provide a potential
 14 | adversary with information that would allow it to determine how, when, and where to most
 15 | effectively execute an attack. Consequently, if this information is released, it will negatively impact
 16 | national security because it could impact the Navy's ability to ensure the operability, reliability,
 17 | safety and security of the TRIDENT missile system.

18 | 23. Incident response force information contains two subcategories of information that
 19 | meet the definition of UCNI. Information in each of these subcategories also meets the definition of
 20 | CISI.

21 | **i. Response Force Personnel Information**

22 | 24. Incident response force information includes incident response force personnel
 23 | information, which may include a comprehensive list of data about the personnel responsible for
 24 | coordinating a response to a radiological incident (e.g., name, title, organization or subunit, position,
 25 | assigned duty, or contact information). The information in these documents qualifies as UCNI,
 26 | pursuant to 223.7(c)(6), "Threat Response Capability and Procedures," because it reveals the
 27 | composition and roles of the incident response force. For example, document 12 identifies the
 28 | federal, state, and local personnel responsible for the coordinated response to a nuclear weapon
 incident, and also identifies the role of each individual in the coordinated response. Although

document 95 identifies the team of personnel (and their organizations and contact information) designated to support the planning of NUWAIX15, anyone reading this information would likely assume (correctly) that these same personnel could be responsible for the coordinated response in the event of an actual radiological event. This information also meets the adverse effects test under 10 U.S.C. § 128 because, in the wrong hands, it could be exploited in the ways discussed above to significantly increase the likelihood of the theft, diversion, or sabotage of DoD SNM, SNM equipment, SNM facilities, or nuclear weapons in DoD custody.

ii. Response Force Location or Capabilities and Threat Scenarios

25. A second type of incident response force information includes information pertaining to the location or capabilities of incident response force personnel, assets or equipment. For example, locating information might include the physical location of command and control operations, telecommunications equipment, or ammunitions stores. Information about incident response force capabilities includes the composition of the incident response force, tactics used in response to threat scenarios, and response times. It also includes information about the assets and equipment used by the incident response force, such as radio communications equipment and frequencies, amounts and type of armaments, and means of transportation.

26. The types of information included in this subcategory are often found together in the responsive records, but there are instances in which this is not the case. For example, document 8 outlines response times and response activities, but does not discuss nuclear weapon incident threat scenarios. Document 15, NUWAIX13 MSEL includes all of types of information in this subcategory—e.g., response activities, response timing and threat scenarios. Document 171, an After Action Report, identifies threat scenarios and key response activities, as well as the key objectives of Federal law enforcement organizations and the vulnerabilities identified as a result of the exercise.

27. Information pertaining to the location or capabilities of incident response force personnel, assets or equipment clearly qualifies for the “Threat Response Capability and Procedures” category in 32 C.F.R. § 223.7(c)(6); in some instances it also falls within the “Vulnerability Assessments” category in 32 C.F.R. § 223.7(c)(1). This information also meets the adverse effects test under 10 U.S.C. § 128 because, in the wrong hands, it could be exploited in the ways discussed above to significantly increase the likelihood of the theft, diversion, or sabotage of DoD SNM, SNM

1 equipment, SNM facilities, or nuclear weapons in DoD custody through a degraded response
2 capability.

3 28. Incident response force information that falls under either subcategory of UCN
4 discussed above, also meets the definition of CISI, under 10 U.S.C. § 130e, and should be protected
5 because the public interest considerations in disclosing this information are strongly outweighed by
6 the harm. Although records containing incident response force information are shared with the
7 County, this information, in the wrong hands, could be used to threaten the security of the
8 installation, and to harm persons and property on the installation and in nearby communities. The
9 ultimate purpose of the incident response force, exercises such as NUWAIX, and the NWIRT
10 Program, is to protect people and property from the harm that could result from an incident, accident,
11 or breach of security. I can think of no compelling public interest that would be served by releasing
12 this information. I recognize that the public has an interest in the release of information pertaining to
13 emergency response plans, such as evacuation plans in the vicinity of the base, in connection with a
14 radiological event on Naval Base Kitsap. However, the incident response force information that the
15 Navy seeks to protect, including incident response force personnel and specific response capabilities,
16 will in no way further this interest. Conversely, releasing this information to the public could
17 increase the likelihood of a radiological event, and thereby prove detrimental to the public interest,
18 by, for example, provoking an attack or increasing the probability of a successful attack, for which
19 emergency response plans, including evacuation plans, are designed to address. Based on this
20 determination, DON has submitted a request to the DoD(DA&M) for a formal determination that the
21 information is CISI, and therefore, remains in the control of DON. As of the date of signing of this
22 declaration we anticipate the CISI process to be completed by late January.

23 29. Finally, I also believe that convoy route and incident response force information meets
24 the definition of information exempt from release under the PRA Security Exemption. *See* RCW
25 42.56.420. The very purpose of the NWIRT program and NUWAIX is to prepare, assess, plan, and
26 prevent or mitigate a nuclear weapon incident (e.g., a terrorist attack). In this case, the records were
27 prepared as part of a coordinated effort, including federal, state and local agencies, in order to prepare
28 for and mitigate the consequences of a radiological incident. For the reasons stated above, if this
information were to fall into the wrong hands, it would constitute a substantial threat to public safety.
These records consist of specific and unique vulnerability assessments or specific and unique

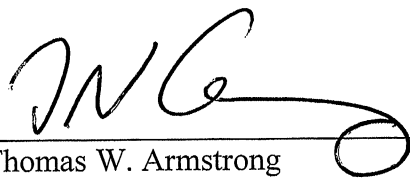
1 response or deployment plans, including compiled underlying data collected in preparation of or
2 essential to the assessments, or to the response or deployment plans; and records not subject to public
3 disclosure under federal law that are shared by federal or international agencies, and information
4 prepared from national security briefings provided to state or local government officials related to
5 domestic preparedness for acts of terrorism. Further, because the information relates to the
6 TRIDENT missile system, if released, it could impact the Navy's ability to ensure the operability,
7 reliability, safety and security of this System, which could negatively impact national security.

8 IV. CONCLUSION

9 30. In summary, SSP conducts TRIDENT missile transport and handling operations and
10 maintains critical specialized support infrastructure at SWFPAC with the utmost care to ensure the
11 security of the base and the health and safety of personnel on the base and the public in the
12 surrounding environment. Although only examples are provided in this declaration, SSP has
13 thoroughly reviewed all of the documents responsive to the PRA request and has determined that
14 each of the documents it marked for redaction contains information that meets the definitions of
15 UCNI, provided in 10 U.S.C. § 128, and CISI, provided in 10 U.S.C. § 130e. SSP also believes that
16 this information meets the definition of information exempt from release under the PRA Security
17 Exemption. I strongly believe that the release of such sensitive information would jeopardize SSP
18 operations on Naval Base Kitsap and the health and safety of DoD employees and the local public,
19 and ultimately pose a risk to national security.

20 Pursuant to 28 U.S.C. §1746, I declare under penalty of perjury under the laws of the United
21 States of America that the foregoing is true and correct to the best of my knowledge, information and
22 belief.

23 Executed the 14th day of December, 2015, at the Washington Navy Yard, Washington DC.

24
25 
26 Thomas W. Armstrong
27 Captain, U.S. Navy
28